PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-337863
(43)Date of publication of application : 07.12.2001

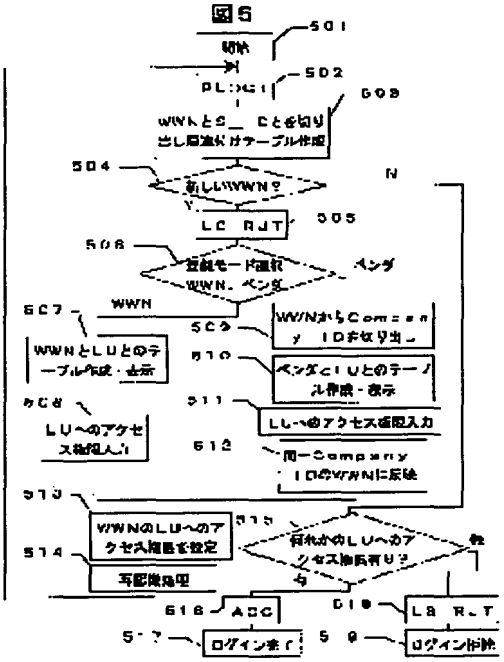
(51)Int.Cl. G06F 12/14
G06F 3/06

(21)Application number : 2000-157954
(22)Date of filing : 24.05.2000

(71)Applicant : HITACHI LTD
(72)Inventor : KAMANO HISAMITSU
TAKAMOTO KENICHI

(54) STORAGE CONTROLLER, STORAGE SYSTEM, AND THE METHOD FOR SETTING SECURITY FOR STORAGE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To readily authorize or inhibit an access to a storage area under the control of a storage controller, by automatically resistering connected host computers.
SOLUTION: By obtaining N-Port-Name information (503) included in a login from a host computer (502) and displaying the information in the state of a table marking access permission both of an subordinate LU and of the host computer (507), an administrator can create security tables of the storage controller only by setting flag information for or against the access (508).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

記憶制御装置及び記憶システム並びに記憶システムのセキュリティ設定方法

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－337863
（P2001－337863A）
(43)公開日　平成13年12月７日(2001.12.7)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｋ　５Ｂ０１７
3/06	３０１	3/06	３０１Ｂ　５Ｂ０６５
	３０４		３０４Ｈ

審査請求　未請求　請求項の数17　ＯＬ　（全 11 頁）

(21)出願番号　特願2000－157954(P2000－157954)

(22)出願日　平成12年５月24日(2000.5.24)

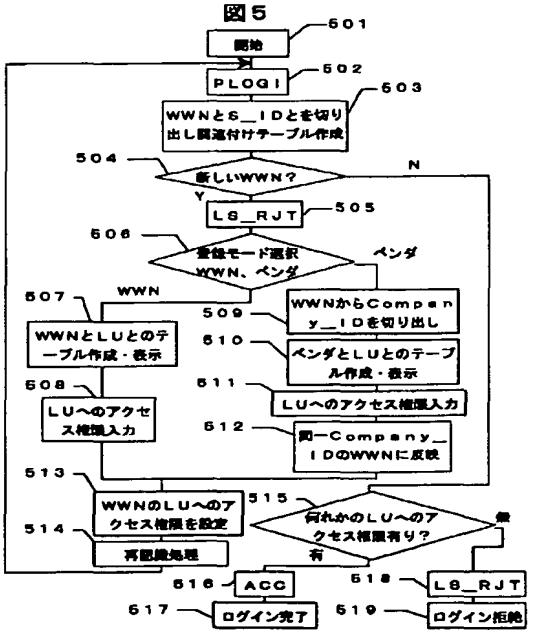
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　鎌野　寿充
神奈川県小田原市国府津2880番地　株式会社日立製作所ストレージシステム事業部内
(72)発明者　高本　賢一
神奈川県小田原市国府津2880番地　株式会社日立製作所ストレージシステム事業部内
(74)代理人　100075096
弁理士　作田　康夫

Ｆターム(参考)　5B017 AA01 BA06 BB06 CA01
5B065 BA01 CA11 CA12 PA12 PA13

(54)【発明の名称】　記憶制御装置及び記憶システム並びに記憶システムのセキュリティ設定方法

(57)【要約】
【課題】接続された上位装置を自動的に登録することにより、簡易に記憶制御装置配下にある記憶領域へのアクセスの許可・抑止を行えることを提供する。
【解決手段】上位装置からのログイン（５０２）に含まれるＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を取得し（５０３）、配下のＬＵと上位装置とのアクセス権限を示すテーブルの状態で管理者に表示する（５０７）ことにより、管理者はアクセス可否のフラグ情報設定（５０８）のみで記憶制御装置のセキュリティテーブルを作成できる。

図５



【特許請求の範囲】

【請求項１】データを記憶する記憶領域を有する記憶装置と、

この記憶装置とのデータ転送を制御するバックエンド制御部と、前記記憶装置から読み出した情報を一時的に格納するキャッシュと、このキャッシュと上位装置との間のデータ転送を制御するフロントエンド制御部と、前記上位装置より送られてきたフレームからこの上位装置を識別する情報を入手しメモリに記憶させるプロセッサとを有する記憶制御装置と、を備えた記憶システム。

【請求項２】データを記憶する記憶領域を有する記憶装置と、

この記憶装置の記憶領域を認識する手段と、上位装置からのログイン要求に含まれるフレームから前記上位装置を識別する情報を分離する手段と、この分離した情報を元に接続されている上位装置と前記記憶領域とを表示するモニタと、この表示に基づき前記上位装置がアクセス可能な前記記憶領域を入力するパネルと、この入力に基づき、前記上位装置の前記記憶領域に対するアクセス権限を設定する手段と、を有する記憶制御装置と、を備えた記憶システム。

【請求項３】前記上位装置を識別する情報は、Ｎ＿Ｐｏｒｔ＿ＮａｍｅまたはＷｏｒｌｄＷｉｄｅ Ｎａｍｅである請求項１又は２記載の記憶システム。

【請求項４】前記上位装置を識別する情報は、Ｃｏｍｐａｎｙ＿ＩＤである請求項１又は２記載の記憶システム。

【請求項５】前記Ｃｏｍｐａｎｙ＿ＩＤに対応するベンダの情報を予め記憶しておく請求項４記載の記憶システム。

【請求項６】前記上位装置を識別する情報は、上位装置のプロトコル、ファイル形式またはＯＳの何れかである請求項１又は２記載の記憶システム。

【請求項７】前記記憶制御装置は前記上位装置とネットワークを介して接続される請求項１乃至６の何れか記載の記憶システム。

【請求項８】前記記憶制御装置は異なったプロトコル及び／または異なったファイルシステムを持つ複数の前記上位装置と接続される請求項１乃至６の何れか記載の記憶システム。

【請求項９】配下の記憶装置とのデータ転送を制御するバックエンド制御部と、前記記憶装置から読み出した情報を一時的に格納するキャッシュと、このキャッシュと上位装置との間のデータ転送を制御するフロントエンド制御部と、前記上位装置より送られてきたフレームからこの上位装置を識別する情報を入手しメモリに記憶させるプロセッサとを有する記憶制御装置。

【請求項１０】配下の記憶領域を認識する手段と、上位装置からのログイン要求に含まれるフレームから前記上位装置を識別する情報を分離する手段と、この分離した情報を元に接続されている上位装置と前記記憶領域とを表示するモニタと、この表示に基づき前記上位装置がアクセス可能な前記記憶領域を入力するパネルと、この入力に基づき、前記上位装置の前記記憶領域に対するアクセス権限を設定する手段と、を有する記憶制御装置。

【請求項１１】上位装置を識別する情報を含んだフレームを受信するステップと、

前記フレームから前記情報を分離して記憶するステップと、

記憶制御装置配下の記憶領域を認識するステップと、

前記分離した情報を元に前記上位装置と前記記憶領域とのテーブルを作成するステップと、

前記テーブルに前記上位装置がアクセス可能な前記記憶領域を入力させるステップと、を備えた記憶システムのセキュリティ設定方法。

【請求項１２】ログイン要求を受信するステップと、

前記ログイン要求に含まれるフレームから上位装置を識別する情報を分離するステップと、

記憶制御装置配下の記憶領域を認識するステップと、

前記分離した情報を元に接続されている上位装置と前記記憶領域とを表示するステップと、

この表示に基づき前記上位装置がアクセス可能な前記記憶領域を入力させるステップと、

この入力に基づき、前記上位装置の前記記憶領域に対するアクセス権限を設定するステップと、を備えた記憶システムのセキュリティ設定方法。

【請求項１３】前記上位装置を識別する情報は、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ，Ｗｏｒｌｄ Ｗｉｄｅ Ｎａｍｅ，Ｃｏｍｐａｎｙ＿ＩＤの何れかである請求項１２記載のセキュリティ設定方法。

【請求項１４】ＰＬＯＧＩを受信するステップと、

このＰＬＯＧＩに含まれるフレームからＮ＿Ｐｏｒｔ＿Ｎａｍｅ又はＷｏｒｌｄ Ｗｉｄｅ Ｎａｍｅを分離するステップと、

このＮ＿Ｐｏｒｔ＿Ｎａｍｅ又はＷｏｒｌｄ Ｗｉｄｅ Ｎａｍｅと前記ＰＬＯＧＩに含まれるＳ＿ＩＤとを関連つけるテーブルを作成するステップと、

前記Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ又はＷｏｒｌｄ Ｗｉｄｅ Ｎａｍｅが予め記憶されているものか判断するステップと、

前記判断により予め記憶されたものでない場合に、記憶制御装置配下の記憶領域を認識するステップと、

前記分離したＮ＿Ｐｏｒｔ＿Ｎａｍｅ又はＷｏｒｌｄ Ｗｉｄｅ Ｎａｍｅを元に接続されている上位装置と前記記憶領域とを表示するステップと、

この表示に基づき前記上位装置がアクセス可能な前記記憶領域を入力させるステップと、

この入力に基づき、前記上位装置の前記記憶領域に対するアクセス権限を設定するステップと、

前記上位装置に再度ＰＬＯＧＩを発信させるステップ

と、を備えた記憶システムのセキュリティ設定方法。

【請求項１５】前記アクセス可能な前記記憶領域の入力は、リードコマンドのアクセスとライトコマンドのアクセスとを別個に行なう請求項１１乃至１４の何れか記載の記憶システムのセキュリティ設定方法。

【請求項１６】ログイン要求を受信するステップと、
前記ログイン要求に含まれるフレームからＷｏｒｌｄ Ｗｉｄｅ Ｎａｍｅを分離するステップと、
このＷｏｒｌｄ Ｗｉｄｅ Ｎａｍｅから更にＣｏｍｐａｎｙ＿ＩＤを分離するステップと、
同一Ｃｏｍｐａｎｙ＿ＩＤと記憶領域とのアクセス権限が既に登録されている場合に、前記アクセス権限を前記ログイン要求を行なった上位装置のアクセス権限とするステップと、を備えた記憶システムのセキュリティ設定方法。

【請求項１７】前記アクセス権限を、前記上位装置に転送するステップを有する請求項１１乃至１６の何れか記載のセキュリティ設定方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置間での不正アクセス防止を行なうセキュリティ設定に関する。具体的には上位装置（ホストコンピュータ）と記憶制御装置（記憶システム）との間にネットワークを構成したコンピュータシステムにおいて、記憶制御装置配下にある記憶領域へのアクセス要求があった際の、不正アクセス防止を行う記憶システム及びこの記憶システムを含むコンピュータシステムに関連する。

【０００２】

【従来の技術】ＡＮＳＩ Ｘ３Ｔ１１で標準化されたファイバチャネルプロトコルでは、多数の装置が接続可能であり、かつＳＣＳＩ、ＥＳＣＯＮ、ＴＣＰ／ＩＰ等多種のプロトコルを同時に運用可能な利点がある。しかし、異種プロトコルのため等異なるファイルシステムによるアクセスによって記憶装置のデータが破壊される恐れが生じる等の問題に対し、セキュリテイ確保等の対策を行なう必要性が発生する。

【０００３】このセキュリティ確保としては、特開平１０－３３３８３９号公報に記載のように、記憶制御装置配下の記憶領域に対するアクセスを許可するために、上位装置を一意に識別する情報と記憶領域へのアクセス可否を表すテーブルを記憶制御装置内に設定しておき、アクセス時にこのテーブルを比較することで、アクセス可能な上位装置以外からのアクセスを拒絶することで不正アクセスを防止する技術がある。

【０００４】この識別情報とはホストバスアダプタ毎に固有なＮ＿Ｐｏｒｔ＿Ｎａｍｅ或いはWWN（World Wide Name）と呼ばれる４８ビットの数字の羅列である。上位装置の識別情報を記憶制御装置内に予め登録しておくことにより、上位装置は記憶制御装置配下にある記憶装置内の記憶領域にアクセスすることができる。

【０００５】

【発明が解決しようとする課題】上位装置の識別情報を記憶制御装置内に予め登録しておくため、ユーザ或いは管理者は、上位装置とＬＡＮで接続されたマネージャ等により、上位装置に固有な８バイトの領域を持ち４８ビットの数字で表されるＮ＿Ｐｏｒｔ＿Ｎａｍｅを調査する。そしてこの数字を控えるなどした後に、自らの手で記憶制御装置へ登録する必要がある。そのため、この登録の際に上位装置のＮ＿Ｐｏｒｔ＿Ｎａｍｅを入力ミスし、意図した上位装置が記憶領域にアクセス出来なかったり、逆に意図しない上位装置が記憶領域にアクセスしデータを破壊してしまう恐れがある。

【０００６】また、多数台の上位装置に対するアクセス可否を登録する場合、非常に時間を要することになる。従って、識別情報の取得および設定に関して、簡易に扱うことが望まれる。

【０００７】本発明の目的は、接続された上位装置を一意に識別する情報を取得し、自動的に記憶制御装置内に登録することにより、簡易に記憶制御装置配下にある記憶領域へのアクセスの許可・抑止を行えるシステムを提供することにある。

【０００８】

【課題を解決するための手段】上記目的を解決するために本発明は、はじめに上位装置から送信されてくるフレーム内に格納された上位装置を識別する情報を取得し、記憶制御装置内に登録し、管理者がアクセスを許可する上位装置についてアクセスを許可するフラグ情報の設定を変更する。

【０００９】

【発明の実施の形態】以下、本発明の実施例について図面を用いて説明する。

【００１０】まず、本発明の対象となる記憶システムとして記憶制御装置と磁気ディスク装置、この記憶システムと上位装置との間にファイバチャネルを用いて構築したネットワークを用いて構成したコンピュータシステム、いわゆるＳＡＮ（StorageArea Network）環境におけるコンピュータシステムについて説明する。

【００１１】ファイバチャネルとは、独自のコマンドセットを持たないシリアルの転送方式をもつプロトコルであり、情報を非同期に送るために伝送媒体の帯域幅を有効に利用できる特色を持っている。そして独自のコマンドセットを持たないかわりに、物理転送方式を、ＳＣＳＩ、ＥＳＣＯＮといったコマンドセットの運搬路として使用することにより、従来のソフトウェア資産を継承しながら、より高速かつ多彩なデータ転送を可能としている。

【００１２】図１は、本発明のコンピュータシステムのハードウェア構成図である。図１において、上位装置１０，２０，３０はデータ処理を行う中央処理装置として

の役割を果たす。複数の磁気ディスクドライブ５０は、記憶制御装置４０の配下にアレイ状に接続される記憶媒体からなる記憶装置である。記憶制御装置４０はこの磁気ディスクドライブ５０の制御を行なうディスクアレイ装置である。

【００１３】記憶制御装置４０は、上位装置１０，２０，３０との間のファイバチャネルプロトコルを制御するフロントエンド制御部（チャネルアダプタ）４１、記憶制御装置４０全体を制御するマイクロプロセッサ４２、記憶制御装置４０の動作を制御するマイクロプログラム及び制御用データ並びに後述する各テーブルを格納する不揮発の制御メモリ４３、データを一時的に格納（バッファリング）しておくキャッシュ４５、このキャッシュへ４５のデータの読み書きを制御するキャッシュ制御部４４、磁気ディスクドライブ５０との間に使用されているプロトコルを制御し、磁気ディスクドライブ５０とのデータデータ転送を制御するバックエンド制御部（ディスクアダプタ）４６、情報設定を行うパネル４７から構成される。

【００１４】磁気ディスクドライブ５０は、論理的に分割した区画に分けられる。ＳＣＳＩのプロトコルでは、この区画をＬＵ（Logical Unit）といい、その領域は、各々、ＬＵＮ（Logical Unit Number）という番号を持つ。本実施の形態では、ＬＵＮ０番のＬＵであるＬＵ０（５１）と、ＬＵＮ１番のＬＵであるＬＵ１（５２）との２つの領域を有する場合を示している。

【００１５】上位装置１０，２０，３０と記憶制御装置４０は、ファイバチャネル６０をインタフェースとし、ファブリック（Fabric）というスイッチ装置を介して接続されている。

【００１６】図１のシステムの動作を、上位装置１０が記憶制御装置４０を経由してディスクドライブ５０内に構成されたＬＵ０（５１）とデータ転送を行う場合を例にとって説明する。上位装置１０が記憶制御装置４０にログインし、その後ＬＵ０（５１）に対してアクセス要求（Ｉ／Ｏ要求）を出すと、その要求を受けたフロントエンド制御部４１はマイクロプロセッサ４２に割込み要求を行う。マイクロプロセッサ４２は、上位装置１０からのコマンド情報や上位装置１０を認識する情報を制御メモリ４３に格納する。上位装置１０がＬＵ０（５１）に対してアクセスが許可されている場合は、コマンド情報を確認する。

【００１７】確認したコマンドがリードコマンドであった場合、マイクロプロセッサ４２は、アクセス要求のあったデータブロックがキャッシュ４５にあるか否かを判断する。該当データがある場合にはそのデータを上位装置１０に転送し、上位装置１０に完了報告を行う。該当データが無い場合には、バックエンド制御部４６を使って、アクセス要求のデータブロックをＬＵ０（５１）から読み出し、キャッシュ制御部４４を使ってキャッシュ４５へデータを格納する。次にマイクロプロセッサ４２は、フロントエンド制御部４１を使って、キャッシュ４５に格納したデータを上位装置１０に転送し、上位装置１０に完了報告を行う。

【００１８】確認したコマンドがライトコマンドであった場合、マイクロプロセッサ４２は、ライト要求のデータブロックをキャッシュ４５に格納し、上位装置１０に完了報告を行う。その後、キャッシュ制御部４４を使ってＬＵ０（５１）へデータを転送し書き込みを終了する。

【００１９】ファイバチャネルがデータをやりとりする基本単位をフレームと言う。次に、このフレームについて、図２を用いて説明する。図２に示すように、フレーム７０はスタートオブフレームＳＯＦ（Start Of Frame）７１、リンク動作の制御やフレームの特徴づけを行う24バイトのフレームヘッダ７２、実際に転送される目的となるデータ部分であるデータフィールド７３、4バイトのサイクリックリダンダンシチェックＣＲＣ（Cyclic Redundancy Check）７４、およびエンドオブフレームＥＯＦ（End Of Frame）７５で構成される。データフィールド７３は０～２１１２バイトの間で可変である。

【００２０】ＳＯＦ７１は、フレームの先頭に置く４バイトの識別子である。ＥＯＦ７５は、フレームの最後につける４バイトの識別子で、ＳＯＦ７１とＥＯＦ７５によりフレームの境界を示す。ファイバチャネルではフレームがないときはアイドル（idle）という信号が流れている。フレームヘッダ７２のフォーマット８０を図３に示す。

【００２１】フレームヘッダの構造について説明する。０ワードの２３－０ビット領域にあたるデスティネーションアイデンティファイＤ＿ＩＤ（Destination ID）８１はフレーム受け取り側のアドレス識別子である。また、１ワードの２３－０ビット領域にあたるソースアイデンティファイＳ＿ＩＤ８２は、フレームの送信先ポートを識別する３バイトのアドレス識別子であり、送受信されるすべてのフレームで有効な値を持つ。そして上位装置を動的に一意に識別できる情報であり、ＰＬＯＧＩ時（後述）に上位装置より報告される値である。このＳ＿ＩＤ８２はシステム立ち上げ毎等に動的に変動する値であり、ＦＣ－ＰＨ（Fibre ChannelPhysical and Signaling Interface：ファイバチャネルの米国標準規格）ではファブリックによって初期化手続き時に割り当てられることになっている。割り当てられる値は、それぞれのポートが持つＮ＿Ｐｏｒｔ＿Ｎａｍｅ、Ｎｏｄｅ＿Ｎａｍｅに依存する。

【００２２】フレームは機能に基づいてデータフレームと制御フレームとに大別される。データフレームは、情報を転送するために用い、データフィールドのペイロード部に上位プロトコルで使用するデータ、コマンドを搭載する。一方、リンク制御フレームは、一般に、フレー

ム配信の成功あるいは不成功を示すのに使われる。フレームを１個受信したことを示したり、ログインする場合に転送に関するパラメータを通知したりするフレーム等がある。

【００２３】次に、「シーケンス」について説明する。ファイバチャネルにおけるシーケンスは、あるＮ＿Ｐｏｒｔから別のＮ＿Ｐｏｒｔへ、一方向に転送されるデータフレームの集まりのことをいい、ＳＣＳＩのフェーズに相当する。シーケンスの集まりをエクスチェンジと呼ぶ。例えば、コマンドを発行して、そのコマンドの終了までに、そのコマンド実行のためにやりとりされるシーケンスの集まり（コマンド発行、データ転送、終了報告）がエクスチェンジとなる。このように、エクスチェンジはＳＣＳＩのＩ／Ｏに相当する。ファイバチャネルインタフェースでは、上位装置がデバイスに対して、通信パラメータを含むポートログインＰＬＯＧＩ（Ｎ＿Ｐｏｒｔ Ｌｏｇｉｎ）コマンドのフレームを送り、デバイスがこれを受け付けることで通信が可能となる。これをログインという。

【００２４】何れかの上位装置から記憶制御装置４０への通信要求であるＰＬＯＧＩフレームの構造について説明する。データフィールド７３の詳細構造において、先頭から２０バイト目～２７バイト目（５～６ワード目）までの８バイトの領域がＮ＿Ｐｏｒｔ＿Ｎａｍｅを格納する領域であり、先頭から２８バイト目～３５バイト目（７～８ワード目）までの８バイトの領域がＮｏｄｅ＿Ｎａｍｅを格納する領域である。

【００２５】デバイスは、要求を受け付ける場合はアクセプトＡＣＣ（Accept）と呼ばれるフレームを、要求を拒絶する場合はリンクサービスリジェクトＬＳ＿ＲＪＴ（LinkService Reject）フレームを、それぞれ、上位装置に送る。

【００２６】図４にログインシーケンス１００を示す。ログイン要求元である上位装置は、ＰＬＯＧＩフレームをログイン要求先であるデバイスの記憶制御装置４０へ送信する。このＰＬＯＧＩフレームには、そのフレームヘッダ７２内にはＳ＿ＩＤ８２及びその他の情報が、データ・フィールド７３内にログイン要求元のＮ＿Ｐｏｒｔ＿Ｎａｍｅ、Ｎｏｄｅ＿Ｎａｍｅが含まれている。

【００２７】記憶制御装置４０では、このフレームに含まれている情報を取り出し、ログインを受諾する場合はＡＣＣフレームをログイン要求元に対して送信する。ログインを拒絶する場合は、ＰＬＯＧＩフレームに対して、記憶制御装置４０はＬＳ＿ＲＪＴと呼ばれるフレームを上位装置に対して送信する。

【００２８】次に、本発明によるセキュリティ情報の取得ならびに自動登録について図５を用いて説明する。

【００２９】周辺装置である記憶制御装置４０等を先に立ち上げた後で、上位装置１０，２０，３０を立ち上げる（ステップ５０１）。各上位装置は、各々のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を格納したログイン要求フレームであるＰＬＯＧＩフレームを発行する。

【００３０】上位装置が追加された場合には、ＰＬＯＧＩの代わりにＦＬＯＧＩ（ファブリックログイン）の処理がスイッチ装置との間で行われた後、スイッチ装置は接続されたデバイスすべてに対して状態に変化が生じたことを示すＲＳＣＮ（Registered State Change Notification）を通知する。そして追加された上位装置に対してＧＰＮ＿ＩＤ（Get Port Name）を送信し、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報を要求する。（ステップ５０２）。記憶制御装置４０のマイクロプロセッサ４２は、フロントエンド制御部４１のポートＰ０を経由してＮ＿Ｐｏｒｔ＿Ｎａｍｅの含まれたフレームを受領する。尚図面においてはＮ＿Ｐｏｒｔ＿Ｎａｍｅの代わりにWWN（World Wide Name）を使用している。WWNはＮ＿Ｐｏｒｔ＿Ｎａｍｅ同様、各装置固有の８バイトの値であり、ポート毎に固有なＰｏｒｔ＿Ｎａｍｅと、ノード毎に固有なＮｏｄｅ＿Ｎａｍｅとの和集合である。

【００３１】後述する実際のＩ／Ｏ要求時（Ｉｎｑｕｉｒｙ）のフレームには、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅが付加されておらず、立ち上げ毎に値が変化するＳ＿ＩＤのみが付加される。そこでマイクロプロセッサ４２は、ＰＬＯＧＩのフレームヘッダからＳ＿ＩＤを、データ・フィールドからＮ＿Ｐｏｒｔ＿Ｎａｍｅを切り出し、ＩｎｑｕｉｒｙにＳ＿ＩＤからＮ＿Ｐｏｒｔ＿Ｎａｍｅを引き出せるように関連付けた、図６（ａ）に示す様な上位装置情報テーブル２００を作成して制御メモリ４３内に格納しておく（ステップ５０３）。

【００３２】次に、マイクロプロセッサ４２は、ステップ５０３にて切り出したWWNが制御メモリ４３内の上位装置情報テーブル２００に登録されているWWNと一致するか否かを確認する（ステップ５０４）。

【００３３】新規のWWNだった場合には、セキュリティテーブルへの登録が行なわれていないために、そのＰＬＯＧＩを発行した上位装置に接続を拒絶するリジェクトパラメータをいれたＬＳ＿ＲＪＴを応答し、拒絶を行なう。（ステップ５０５）。そして新しい上位装置が接続されたものと認識し、パネルの表示部に新しい上位装置が接続された旨を表示し、セキュリティテーブルへの登録を行なうためのモード選択を管理者に促す。選択できるモードとしては、WWNそのものを使用して登録するモードと、WWN内に含まれるＣｏｍｐａｎｙ＿ＩＤを用いて登録するモードとを備える（ステップ５０６）。尚、新しい上位装置が接続された旨は、画面の点滅や音声による案内等、管理者が認識しやすい表示の仕方とする。

【００３４】Ｃｏｍｐａｎｙ＿ＩＤについて説明する。Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ８バイトは、その６０～６３ビットの４ビットエリアに識別フィールドを、３６～５９ビットの２４ビットエリアにＣｏｍｐａｎｙ＿ＩＤを、

０～３５ビットの３６ビットエリアにＶＳ＿ＩＤ（Vendor Specific Identifier）を含んで構成されいる。ここでＣｏｍｐａｎｙ＿ＩＤは、各ベンダ毎にユニークな値が割り振られている。つまり、同じベンダは同じ値を備えている。

【００３５】異なるプロトコルや異なるファイルシステムを持つ上位装置からのＩ／Ｏによるデータ破壊を防止するためのセキュリティでは、同じベンダの上位装置がアクセスできるデバイスは同一である場合が多い。そのため、ベンダ毎のセキュリティを設定しても問題ことが多く、複数台まとめてアクセス可否を設定出来るので、より簡易にセキュリティテーブルの作成が行なえる。

【００３６】管理者がWWN毎（複数の上位装置を登録する場合でも１台毎）の登録を選択した場合、マイクロプロセッサ４２は、装置立ち上げ時等セキュリティテーブルが全く作成されていない場合には、記憶制御装置４０配下の記憶領域であるＬＵを認識する。そして図６（ｂ）に示すような上位装置とＬＵとのセキュリテーブル２０１を作成する。上位装置の追加時や再立ち上げ時等、前もってセキュリティテーブル２０１が存在する場合には、セキュリティテーブル２０１に新しいWWNに相当する上位装置を追加し新しいセキュリティテーブルを作成する。

【００３７】そしてこのセキュリティテーブル２０１をパネル４７の表示部に表示する（ステップ５０７）。管理者は、パネル４７を用いてこのテーブルに上位装置のアクセス可否のみを入力する（ステップ５０８）。

【００３８】入力の仕方の一例を図７に示す。図７はパネル４７を示している。表示部４７１には、自動登録された上位装置（この場合にはＨｏｓｔＡ，ＨｏｓｔＢは既に登録されている上位装置であり、ＨｏｓｔＣが新しく登録された上位装置とする）が表示される。キー部４７２の矢印キーを押すことによってＨｏｓｔＣを選択すると、ＬＵアクセス許可・抑止フラグ情報の設定変更が可能となる。ここで管理者はＥｎａｂｌｅを選択することでアクセスを許可できる。このＬＵアクセス許可・抑止フラグ情報はデフォルトでは、Ｄｉｓａｂｌｅとしておく方が良い。キー部４７２には数字キーも備えることで従来の様にWWNを手入力することも出来る。図７では簡単のため、ＬＵ（記憶領域）が一つの場合の例を示している。

【００３９】管理者がベンダ毎の登録を選択した場合、マイクロプロセッサ４２は、WWNからＣｏｍｐａｎｙ＿ＩＤを切り出す（ステップ５０９）。そしてこのＣｏｍｐａｎｙ＿ＩＤを用いて図６（ｃ）に示すようなベンダとＬＵとのアクセス可否テーブル２０２を（ステップ５０７）と同様にして作成し表示する（ステップ５１０）。管理者は、このテーブルにパネル４７を用いて上位装置のアクセス可否のみを入力する（ステップ５１１）。

【００４０】セキュリティテーブル２０１は上位装置（WWN）とＬＵとの対応を表しているので、ステップ５１１にて作成したアクセス可否テーブル２０２を参考にして、各Ｃｏｍｐａｎｙ＿ＩＤを有する上位装置（WWN）のアクセス可否入力を自動的に行ない、ステップ５０７の代替とする（ステップ５１２）。

【００４１】以上の入力を元にして、セキュリティテーブル２０１を完成させ、設定更新する（ステップ５１３）。

【００４２】この様にして新しいセキュリティテーブル２０１に更新された後、マイクロプロセッサ４２は上位装置にＧＰＮ＿ＩＤ（Get_Port_Name）を発行することで、再度上位装置にＰＬＯＧＩを発行させる（ステップ５１４）。

【００４３】今度は新しいWWNではないのでステップ５０４においてNが選択されステップ５１５に進む。

【００４４】ステップ５０４において、WWNが既知の場合には、ログイン続行し、このWWNが記憶制御装置４０にログイン可能か否かを判断する。そのために、セキュリティテーブル２０１を参照して、このWWNが記憶制御装置４０配下の何れかのＬＵ（図１の場合にはＬＵ０かＬＵ１）にアクセス権限が有るか否かを判断する（ステップ５１５）。

【００４５】アクセス権限が設定されている上位装置には、ＡＣＣを返し（ステップ５１６）、ログインを完了する（ステップ５１７）。

【００４６】アクセス権限がない上位装置には、ＬＳ＿ＲＪＴを返し（ステップ５１８）、ログインを拒絶する（ステップ５１９）。

【００４７】ここで、初期システム立ち上げ時の様に、複数台の上位装置が新しく接続された場合、どの上位装置がどのWWNであるかということを管理者は認識できない。そのため、ステップ５０６において、WWN毎に登録を選択する場合には、別途システムに接続されたＳＡＮマネージャ等からどの上位装置がどのWWNを備えているかをチェックしておくことによって、管理者はアクセス権限の有無を入力するのみでセキュリティテーブル２０１を作成する事が出来る。

【００４８】ここで、ＳＡＮマネージャ装置について図１２を用いて説明する。上位装置１０，２０，３０ならびに記憶制御装置４０はファイバチャネルＦａｂｒｉｃ６０とは別にローカルエリアネットワーク（ＬＡＮ）６１で接続されている。このＬＡＮ６１にはＳＡＮマネージャ装置９０やファイバチャネルＦａｂｒｉｃ６０も接続されている。ＳＡＮマネージャ装置９０はＰＣやＷＳであり、ＬＡＮ６１経由で上位装置１０、２０，３０や記憶制御装置４０ならびにファイバチャネルＦａｂｒｉｃ６０からＳＡＮのシステム構成を表す情報を取得する。

【００４９】また、ステップ５０６において、ベンダ毎

の登録モードを選択した場合に備えて、予め制御メモリ内に各ベンダのＣｏｍｐａｎｙ＿ＩＤを記憶しておくことで、新しいWWNが何れのベンダの上位装置かを知ることが出来る。よって、初期設定時においても管理者はモード選択を行なうのみでアクセス権限の有無を入力することもなく、セキュリティテーブル２０１を作成する事が出来る。

【００５０】次に、Ｉｎｑｕｉｒｙコマンド実行について図８を用いて説明する。Ｉｎｑｕｉｒｙコマンドとは、Ｉ／Ｏプロセスを開始しようとする場合に先立ち、プロセスの対象となる論理デバイスに対して、その実装状態を問い合わせるコマンドである。具体的には、上位装置から記憶制御装置４０配下の記憶領域ＬＵへのアクセス要求に先立つ情報問い合わせ要求のことである。本コマンドはＳＣＳＩでは必ずサポートされている標準コマンドである。

【００５１】フレームヘッダ８０の詳細構造において、ＬＵにアクセスしようとする上位装置は、アクセスしようとするＬＵをもつ記憶制御装置４０に対し、Ｉｎｑｕｉｒｙコマンドを含むフレームを送信する（ステップ８０１）。このフレームには、ＰＬＯＧＩで割り当てられた、上位装置のＳ＿ＩＤ８２と、問い合わせを行うＬＵの識別子であるＬＵＮが含まれている。

【００５２】そしてＩｎｑｕｉｒｙが発行されてＩ／Ｏを行なう際には、ＩｎｑｕｉｒｙフレームよりＳ＿ＩＤ８２を切り出し（ステップ８０２）、Ｎ＿Ｐｏｒｔ＿ＮａｍｅとＳ＿ＩＤ８２とを関連付けたテーブルからＳ＿ＩＤ８２に対応するＮ＿Ｐｏｒｔ＿Ｎａｍｅを求める事で、Ｉｎｑｕｉｒｙが何れの上位装置によって発行されたものかを判定する（ステップ８０３）。

【００５３】そして判定された上位装置がＩ／Ｏを行なうＬＵに対してアクセス権限があるか否かをセキュリティテーブル２０１により判定し（ステップ８０４）、権限がある場合にはアクセスを受付けるためにＩｎｑｕｉｒｙを発行した上位装置に対してＡＣＣを返し（ステップ８０５）、Ｉ／Ｏ処理を行なう（ステップ８０６）。権限がない場合にはＬＳ＿ＲＪＴを上位装置に返し（ステップ８０７）、Ｉ／Ｏ要求を拒絶する（ステップ８０８）。

【００５４】以上のように、Ｉ／Ｏ処理かＩ／Ｏ要求拒絶を行いＩｎｑｕｉｒｙは終了する（ステップ８０９）。

【００５５】次に、図９を用いて、上位装置の登録のみならず、セキュリティ設定までも自動登録するモードを備えた機能を有する実施例を説明する。

【００５６】ステップ９０１から９０９までは、図５に示したステップ５０１から５０９と同一なので説明は省略する。

【００５７】ステップ９０９においてＣｏｍｐａｎｙ＿ＩＤを切り出した後、ユーザはセキュリティ登録を手動で行なうか自動で行なうか選択する（ステップ９１０）。

【００５８】手動を選択した場合、ステップ９１１と９１２とは、図５に示したステップ５１０と５１１と同一なので説明は省略する。

【００５９】自動を選択した場合、マイクロプロセッサ４２は、セキュリティテーブル２００に登録されている上位装置の中に、新しいWWNのＣｏｍｐａｎｙ＿ＩＤと同一のものが有るか否かを検索する。（ステップ９１３）。

【００６０】無い場合には、セキュリティ自動設定は行なう事が出来ないので、手動設定と同様にステップ９１１へ進む。同一Ｃｏｍｐａｎｙ＿ＩＤがある場合には、そのＣｏｍｐａｎｙ＿ＩＤのセキュリティ設定をコピーすることで当該上位装置に対するアクセス可否設定入力を省く（ステップ９１４）。

【００６１】以上のようにして、ベンダ毎のセキュリティテーブルを作成した後のステップ９１５以降は、図５のステップ６１３以降と同様であるので説明は省略する。

【００６２】次に稼動しているコンピュータシステムにおいて、障害等により上位装置の一時停止、或いはホストバスアダプタを交換する場合について、図１０を用いて説明する。

【００６３】ある上位装置がシステムから抜かれた（ステップ１００１）とき、すなわち上位装置に接続されたケーブルをスイッチ装置から抜いたとき、ファイバチャネル６０のスイッチ装置（図示せず）は、接続されたデバイスすべてに対して状態に変化が生じたことを示すＲＳＣＮを通知する（ステップ１００２）。この通知を受信した記憶制御装置４０は、アクセプト（ＡＣＣ）フレームを送信する（ステップ１００３）。記憶制御装置４０は、既にログイン中の上位装置の中にＲＳＣＮで通知のあった上位装置があるかを確認する（ステップ１００４）。あった場合には、その上位装置に対してＧＰＮ＿ＩＤを送信する（ステップ１００５）。

【００６４】上位装置は接続を外されたため、ＧＰＮ＿ＩＤに対する応答をすることができないので、記憶制御装置４０はアクセプト（ＦＳ_ＡＣＣ）を受信することができない（ステップ１００６）。そこで記憶制御装置４０でこの上位装置に対して内部的にログアウト処理を実施する。そしてセキュリティテーブル２００のアクセス許可・抑止フラグ情報を、Ｄｉｓａｂｌｅに変更し、アクセス抑止する（ステップ１００７）。ホストバスアダプタを交換後、スイッチ装置に接続し直すときは、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報が変更になるため、上位装置新設／追加に関する実施例と同様となる。

【００６５】ここで、ステップ１００７においてセキュリティテーブル２００のアクセス許可・抑止フラグ情報の変更を行なわないように設定しておけば、上位装置の

停止が一時的であったり、修理を完了して復帰した場合には、セキュリティテーブル２００の再設定を行なうことなく、停止以前と同じ記憶領域にアクセスする事が出来る。ホストバスアダプタ交換処理は同じポートにおけるケーブルの挿抜処理を行うため、“障害等によるホストアダプタ交換と判断する”モードにしておくと、管理者がパネル４７からアクセスを許可しなくても、アクセスできるように自動設定される（ステップ５１２）。逆に、“アクセス許可・抑止を行う”モードにしておけば、上位装置追加に関する実施例と同じ処理にて、追加処理がなされる。

【００６６】次に図１１を用いてＬＵセキュリティ変更について説明する。パネル４７を用いてセキュリティーテーブルの変更を開始する（ステップ１１０１）。最初は変更モードをWWN毎かベンダ毎かを選択する（ステップ１１０２）。

【００６７】WWN毎を選択した場合には、マイクロプロセッサ４２は、パネル４７の表示部４７１に設定されている上位装置の一覧を示す（ステップ１１０３）。そして管理者は、キー部４７２を用いて変更する上位装置のアクセス可否を変更する（ステップ１１０４）。

【００６８】ベンダ毎を選択した場合には、マイクロプロセッサ４２は、上位装置情報テーブル２００のWWNからＣｏｎｐａｎｙ＿ＩＤを切り出し、ベンダ毎のアクセス可否テーブル２０２作成する（ステップ１１０５）。そしてこのベンダ毎のアクセス可否テーブル２０２をパネル４７の表示部４７１に示す（ステップ１１０６）。管理者は、キー部４７２を用いて変更するベンダのアクセス可否を変更する（ステップ１１０７）。その結果に基づきマイクロプロセッサ４２は、変更したベンダのＣｏｎｐａｎｙ＿ＩＤを持つWWNを検索し、ステップ１１０４と同じ結果となるようにする（ステップ１１０８）。

【００６９】そしてマイクロプロセッサ４２は、セキュリティテーブル２０１を変更する（ステップ１１０９）。そして上位装置に再認識処理を行わせるコマンドを発信し（ステップ１１１０）、上位装置はこのコマンドに対してＰＬＯＧＩを発信することでログインを行なう（ステップ１１１１）。尚、アクセス可能だった上位装置をアクセス不可にするためには、再認識処理の前に記憶制御装置側４０で、内部的にアクセス不可にする上位装置をログアウトさせておく。

【００７０】上記の３例では、記憶制御装置４０のフロントエンド制御部４１のＬＵ単位でのアクセス許可・抑止を行っているが、ＬＵ毎ではなく、記憶制御装置４０毎で設定することも可能であり、その場合にはセキュリティテーブル２０１のアクセス先がＬＵではなく記憶制御装置４０の形式となる。また、フロントエンド制御部４１が複数のポートを持つ場合には、ポート毎に上位装置のアクセス権限を設定する事で、上位装置の競合を避けたり優先度をつける事が可能となる。

【００７１】また、セキュリティテーブル２０１を記憶制御装置４０で作成後に上位装置に転送し、上位装置自身がＰＬＯＧＩやＩｎｑｕｉｒｙを発信する前にアクセス権限が有るか否かを判断することによってセキュリティシステムを構築してもよい。この場合には、上位装置は各記憶制御装置から送られてきたセキュリティテーブルから自身のアクセス権限のところのみを選択して記憶しておけばよい。同様に、上位装置と記憶制御装置の間に位置するスイッチ或いはＳＡＮマネージャ内にセキュリティテーブルを設けてもよい。この様にすることで、ファイバチャネルを転送されるコマンドや、記憶制御装置が処理するコマンドを減少させることが出来、Ｉ／Ｏ処理をより効率的に行なう事が出来る。

【００７２】また、異種プロトコルや異なるファイルシステム、異なるＯＳからのアクセスによるデータ破壊は、通常はデータライト時にのみ発生するものであり、データリードに関しては他のプロトコルや異なるファイルシステムを持つ上位装置からも行なえた方が便利な場合が多い。よって、図５のステップ５０７やステップ５０８の様に、ユーザにアクセス権限を入力させる際にリードアクセスとライトアクセスとを別々に設定させることで、読み出しのみは許可する記憶領域を備えたり、書き込みのみアクセス権限を設けさせるような設定として読み出しは自由に行なえるようにしてもよい。

【００７３】また、同一ベンダが複数のファイル形式の上位装置を製造していることもある。その場合にＣｏｍｐａｎｙ＿ＩＤを使用すると、本来のセキュリティを達成することが出来なくなる恐れがある。そのような場合には、Ｃｏｍｐａｎｙ＿ＩＤにＯＳやファイル形式等を識別しているコードの部分を加えて、先の実施例で説明したＣｏｍｐａｎｙ＿ＩＤの代わりとすることで対応できる。

【００７４】また、上位措置を識別する際にＮ＿Ｐｏｒｔ＿Ｎａｍｅを用いず、ＰＬＯＧＩから上位装置のプロトコルやファイル形式、ＯＳを識別することにより、これらの識別情報をＣｏｍｐａｎｙ＿ＩＤ代わりとすることで、同じファイル形式の上位装置には同一のアクセス権限を与えるような設定とする事が出来る。

【００７５】尚、上記実施例においては説明を簡単にするために記憶制御装置は1台、ＬＵは２つとしたが、複数台の記憶制御装置からなるシステムでも、ＬＵ数が３以上でのシステムであった場合、より本発明を適用する事によりセキュリティー設定を簡易化する事が出来るのは言うまでもない。また、記憶領域としてＬＵ単位でなく、論理ボリューム単位、ＲＡＩＤグループ単位、論理的に区分された単位ではない物理領域或いは物理ボリュームの単位でも設定可能である。また、記憶装置や記憶制御装置が複数台有るものの、論理的には一つの記憶装置や記憶制御装置である場合のように、上位装置、記憶

制御装置、記憶装置が複数台という場合には、論理的に複数及び物理的に複数の何れの意味をも含むものである。

【００７６】また、記憶媒体として磁気ディスクの他に、光ディスクや光磁気ディスク、媒体形状としてはディスク以外にテープ等でも良いし、対象となる技術分野も上位装置と記憶制御装置との間に限らず、アクセス制限を設ける必要の生じる情報処理装置間等に適用できる事はもちろんである。

【００７７】

【発明の効果】以上述べたように、本発明によって、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、記憶制御装置配下にある１つ以上の記憶領域、から構成されるコンピュータシステムにおいて、接続された上位装置を一意に識別する情報を自動的に取得・登録することにより、簡易に記憶制御装置配下にある記憶領域へのアクセスの許可・抑止を行えることができ、管理上の負担を減少させることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態を示すハードウェア構成図である。

【図２】フレームのフォーマットを示す図である。

【図３】フレームヘッダの詳細を示す図である。

【図４】上位装置とデバイス間のログイン時のシーケンス図である。

【図５】ログインとセキュリティテーブル登録・設定とのフローチャートである。

【図６】セキュリティテーブルの一例を示す図である。

【図７】セキュリティ情報登録時の表示部の一例を示す図である。

【図８】Ｉｎｑｕｉｒｙコマンドのフローチャートである。

【図９】セキュリティテーブル自動設定モードを有するフローチャートである。

【図１０】デバイス一時停止の際の処理を示すフローチャートである。

【図１１】セキュリティテーブル変更と再ログインのフローチャートである。

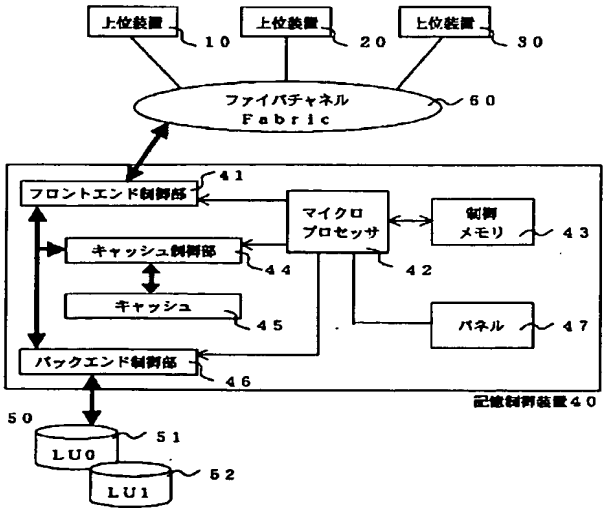
【図１２】ＳＡＮマネージャを示す図である。

【符号の説明】

１０，２０，３０…上位装置、４０…記憶制御装置、４１…フロントエンド制御部、４２…マイクロプロセッサ、４３…制御メモリ、４４…キャッシュ制御部、４５…キャッシュ、４６…バックエンド制御部、４７…パネル、５０…磁気ディスクドライブ、５１…ＬＵ０、５２…ＬＵ１、６０…ファイバチャネル、６１…ローカルエリアネットワーク、７０…フレーム、７１…スタートオブフレーム、７２…フレームヘッダ、７３…データフィールド、７４…サイクリック・リダンダンシチェック、７５…エンドオブフレーム、８０…フレームヘッダ、８１…デスティネーションアイデンティファイア、８２…ソースアイデンティファイア、９０…ＳＡＮマネージャ装置、２００…上位装置情報テーブル、２０１…セキュリティテーブル、２０２…ベンダ毎のアクセス可否テーブル、４７１…表示部、４７２…キー部。

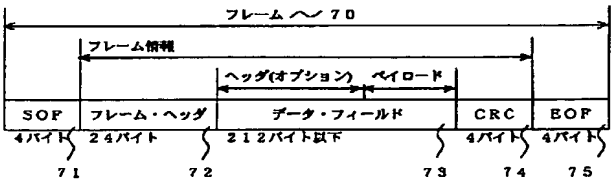
【図１】

図１



【図２】

図２



【図３】

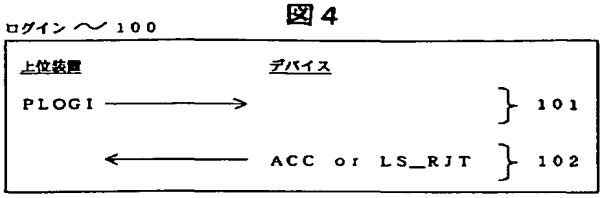
図３

フレームヘッダ 80

Word \ Bit	31－24	23－16	15－8	7－0	
0	R_CTL	D_ID(フレーム受信側のN_Portアドレス識別子)			81
1	Reserved	S_ID(フレーム送信側のN_Portアドレス識別子)			82
2	TYPE	F_CTL			
3	SEQ_ID	DF_CTL	SEQ_CNT		
4	OX_ID		RX_ID		
5	Parameter				

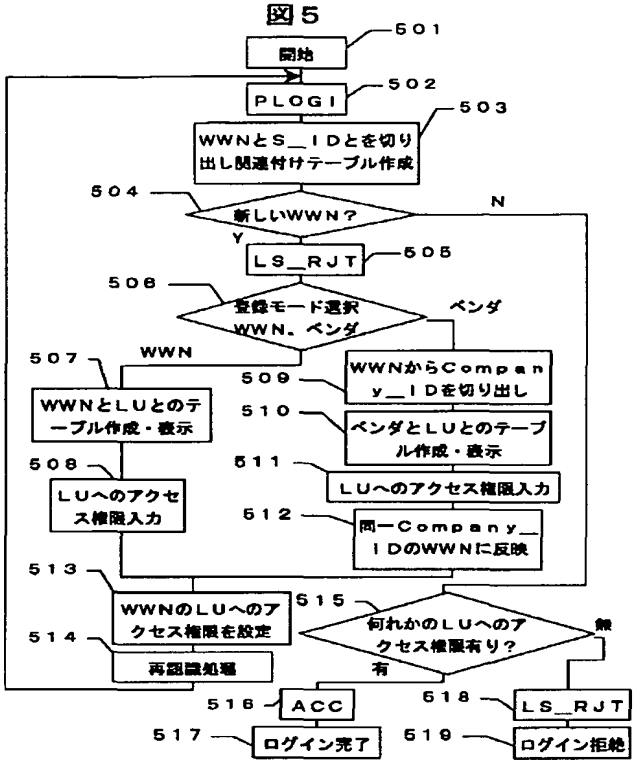
【図４】

図４



【図５】

図５



【図６】

図６

(a)

	WWN	S_ID
HostA	01234567 89ABCDEF	FFFF01
HostB	01234567 89ABCDEE	FFFF02
HostC	01234567 89ABCDED	FFFF03

200

(b)

	アクセス可否	
	LU0	LU1
HostA	不[redacted]	[redacted]
HostB	[redacted]	不[redacted]
HostC	[redacted]	不[redacted]

201

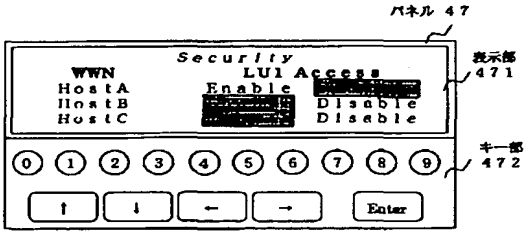
(c)

	アクセス可否	
	LU0	LU1
ベンダA	×	○
ベンダB	○	×

202

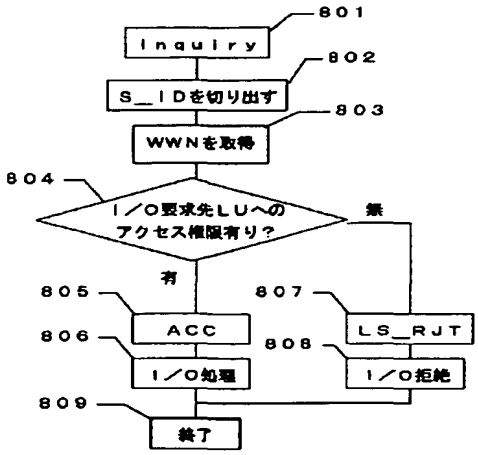
【図７】

図７



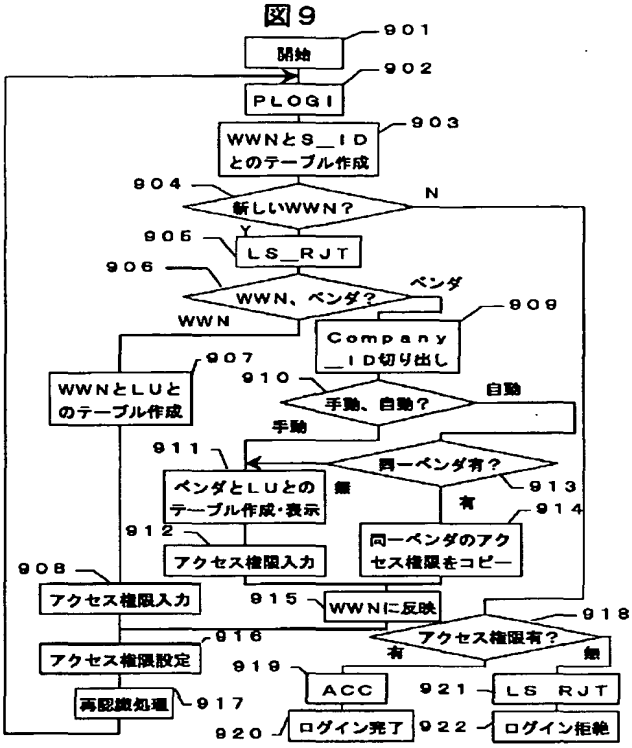
【図８】

図８



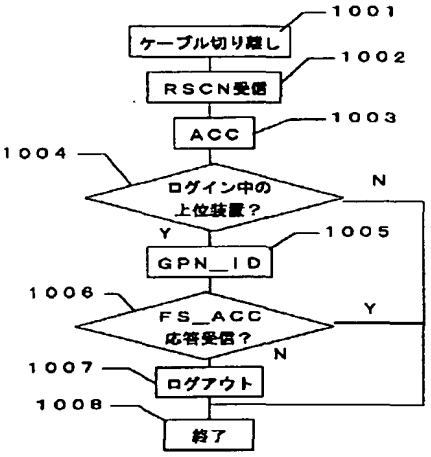
【図９】

図９



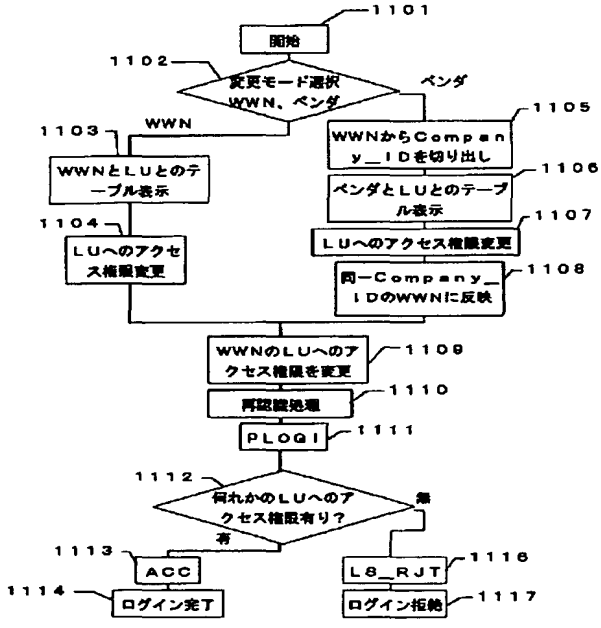
【図１０】

図１０



【図１１】

図１１



【図１２】

図１２